



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,488	11/30/2000	Sunil K. Srivastava	50325-0108 (1590)	4277

29989 7590 04/05/2006

HICKMAN PALERMO TRUONG & BECKER, LLP  
2055 GATEWAY PLACE  
SUITE 550  
SAN JOSE, CA 95110

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/728,488

Applicant(s)

SRIVASTAVA, SUNIL K.

Examiner

Aravind K. Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 03 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) See Continuation Sheet is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,6,10,12,15,16,20,23,24,31,34,38,42,47,48,51,54-56 and 59-101 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_.

Continuation of Disposition of Claims: Claims pending in the application are 1,2,4,6,10,12,15,16,20,23,24,31,34,38,42,47,48,51,54-56 and 59-101.

### **DETAILED ACTION**

1. This is in response to the amendment filed on 3 January 2006.
2. Claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56 and 59-101 are pending in the application.
3. Claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56 and 59-101 have been rejected.
4. Claims 3, 5, 7-9, 11, 13, 14, 17-19, 21, 22, 25-30, 32, 33, 35-37, 39-41, 43-46, 49, 50, 52, 53, 57 and 58 have been cancelled.

#### ***Response to Amendment***

5. The examiner approves of the new abstract. The abstract no longer exceeds the 150-word limit. No new matter has been added.

#### ***Response to Arguments***

6. Applicant's arguments with respect to claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**7. Claims 1, 2, 4-6, 9-32, 34, 35 and 38-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Briscoe U.S. 2003/0044017.**

As to claim 1, Briscoe discloses a method of establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, comprising the steps of:

receiving information defining a plurality of multicast proxy service nodes

[0058], wherein:

the plurality of multicast service nodes are distributed across the wide area network [0058];

the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group [0077]; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree [0114], wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network [0125-0129]; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes [0125-0129];

creating and storing a second binary tree that represents the plurality of member nodes [0125-0129], wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree [0131-0135];

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network [0131-0135];

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes [0131-0135]; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center [0131-0135];

creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange [0131-0135];

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree [0131-0135].

As to claims 2, 61 and 82, Briscoe discloses that each of the member nodes is associated with at least one of the multicast proxy service nodes, wherein each of the multicast proxy service nodes acts as one of a plurality of group controllers, further comprising the steps of:

joining an additional group controller to the plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of another group controller of the plurality of group controllers [0076-0081];

establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol [0076-0081];

receiving a request to add or delete a specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers [0076-0081];

creating and storing the new group session key for each member node in each branch of the second binary tree that is affected by adding or deleting the specified member node from the multicast group [0076-0081];

distributing the new group session key from one of the group controllers to the member nodes that are affected by adding or deleting the specified member node [0076-0081].

As to claims 4, 62 and 83, Briscoe discloses a method wherein distributing a group session key further comprises:

- determining that the specified member node is leaving the multicast group [0085-0103];

- determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is leaving [0085-0103];

- updating only keys associated with the intermediate nodes that are affected by the specified member node that is leaving [0085-0103]; and

- sending the new group session key to the leaf nodes of the second binary tree that correspond to the member nodes that are affected by deleting the specified member node [0085-0103].

As to claims 6, 63 and 84, Briscoe discloses a method wherein distributing a group session key further comprises:

- receiving a request message from the specified member node to join the multicast group [0085-0103];

- determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is joining the multicast group [0085-0103];

- updating only keys associated with the intermediate nodes that are affected by the specified member node that is joining [0085-0103];

- generating a private key for the specified member node that is joining [0085-0103]; and



sending a message comprising the new group session key, the private key, and the updated keys of intermediate nodes that are affected to the member node that is joining [0085-0103].

As to claims 10, 64 and 85, Briscoe discloses that determining a new group session key further comprises the step of computing a group shared secret key at a first member node of the plurality of member nodes for use in a public key process and using less than  $n * (n-1)$  messages, where "n" is a number of member nodes in the multicast group, by the steps of:

generating an intermediate shared secret key by issuing communications to a second member node of the plurality of member [0104-0109];

sending a first private value associated with the first member node to the second member node, and receiving from the second member node a second private value associated with the second member node using the intermediate shared secret key [0104-0109];

generating and communicating a collective public key that is based upon the first private value and the second private value to a third member node of the plurality of member nodes [0104-0109];

receiving an individual public key from the third member node [0104-0109]; and

computing and storing the group shared secret key based upon the individual public key [0104-0109].

As to claims 12, 65 and 86, Briscoe discloses that the step of communicating the collective public key further comprises determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of the first and second member nodes into the multicast group [0061].

As to claims 15, 66 and 87, Briscoe suggests that computing and storing the group shared secret key further comprises the steps of computing and storing a group shared secret key value "k" at the first member node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q) \text{ [0207-0218]}$$

wherein:

C, a, b, c, q, and p are values stored in a memory [0207-0218],

C is the individual public key [0207-0218],

a is the first private value of the first member node [0207-0218],

b is the second private value of the second member node [0207-0218],

c is a third private value of the third member node [0207-0218],

p is a base value [0207-0218], and

q is a prime number value [0207-0218].

As to claims 16, 67 and 88, Briscoe discloses that determining a new group session key comprises computing a group shared secret key, each of the member nodes having a private key value associated therewith, by the steps of:

communicating a first public key of a first member node of the plurality of member nodes to a second member node of the plurality of member nodes [0061-0064];

creating and storing an initial shared secret key for the first member node and the second member node based on a first private key and a second public key that is received from the second member node [0061-0064];

creating and storing information at the first member node that associates the first member node with a first entity by generating a collective public key that is shared by the first member node and the second member node, wherein the collective public key is based on the first private key and a second private key that is derived by the first member node from the second public key [0061-0064];

receiving a third public key from a third member node of the plurality of member nodes that seeks to join the first entity [0061-0064];

creating and storing a final shared secret key based on the collective public key and a third public key [0061-0064];

joining the first member node to a second entity that includes the first entity and the third member node and that uses secure communication with messages that are encrypted using the final shared secret key [0061-0064].

As to claims 20, 68 and 89, Briscoe suggests a method further comprising the steps of creating and storing a subsequent shared secret key for use by the first entity and the third member node to enable the third member node to independently compute the group shared key, that creating and storing the subsequent shared secret key further comprises the steps of creating and storing a subsequent shared secret key value,  $k$ , according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q) \text{ [0207-0218]}$$

where:

$p$  = a random number [0207-0218],

$q$  = a prime number [0207-0218],

$a$  = the first private key [0207-0218],

$b$  = the second private key [0207-0218],

$c$  = a third private key of the third member node [0207-0218],

$x$  = a number of times the first member node has participated in entity formation [0207-0218],

$y$  = a number of times the second member node has participated in entity formation [0207-0218], and

$z$  = a number of times the third member node has participated in entity formation [0207-0218].

As to claims 23, 69 and 90, Briscoe suggests that creating and storing the initial shared secret key for the first member node and second member node further comprises the steps of creating and storing an initial shared public key value "AB" according to the relation

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q) \text{ [0207-0218]}$$

wherein  $k$  = the initial shared secret key value,  $a$  = the first private key value,  $b$  = the second private key value,  $p$  is a base value, and  $q$  is a randomly generated prime number value [0207-0218].

As to claims 24, 70 and 91, Briscoe discloses a method further comprising the steps of:

authenticating a first multicast proxy service node with a subset of the multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on key information stored in a directory [0072-0083];

wherein authenticating the first multicast proxy service node based on key information stored in the directory includes authenticating the first multicast proxy service node based on the directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating attribute information of one or more multicast proxy service nodes, wherein the attribute information comprises the group session key and the private keys of the one or more multicast proxy service nodes [0072-0083];

receiving a plurality of private keys from the subset of multicast proxy service nodes [0072-0083];

generating a new private key for the first multicast proxy service node [0072-0083];

communicating the plurality of private keys and the new private key to the first multicast proxy service node [0072-0083];

communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys [0072-0083];

distributing the new group session key to all multicast proxy service nodes of the plurality of multicast proxy service nodes by:

creating and storing the new group session key using a particular multicast proxy service node of a particular domain of the plurality of domains of the directory service, wherein the particular domain is associated with the directory [0072-0083];

replicating the directory [0072-0083]; and

obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node [0072-0083].

As to claims 31, 71 and 92, Briscoe discloses a method further comprising selectively updating the group session key and the private keys by:

- detecting whether a member node of the plurality of member nodes that is associated with one of the leaf nodes is leaving the multicast group [0110-0112];

- determining one or more tree nodes along a tree path in the second binary tree that corresponds to the leaving leaf node, wherein the one or more tree nodes are affected in response to the detecting step [0110-0112];

- updating the private keys of the one or more tree nodes [0110-0112];

- one of the affected intermediate nodes that is a parent node of the leaving leaf node generating the new group session key and selectively sending the new group session key to all ancestral nodes along the tree path [0110-0112];

- modifying the key information based upon the updated private keys and the new group session key [0110-0112]; and

- generating instructions that distribute the modified key information using directory replication [0110-0112].

As to claims 34, 72 and 93, Briscoe discloses a method further comprising selectively updating a group session key and the private keys, wherein the step of selectively updating comprises:

- receiving a request message from a new member node to join the multicast group [0085-0103];

- determining one or more tree nodes along a tree path in the second binary tree that corresponds to a new leaf node in the second binary tree for the new

member node, wherein the one or more nodes are affected in response to the receiving step [0085-0103];

updating the private keys of the one or more tree nodes [0085-0103];

one of the affected intermediate nodes that is a parent node of the new leaf node requesting permission from a root node of the second binary tree to generate the new session key and generating the new group session key and a private key of the new leaf node [0085-0103];

modifying the key information based upon the updated private keys, the new group session key, and the private key of the new leaf node [0085-0103]; and

generating instructions that distribute the modified key information using directory replication [0085-0103].

As to claims 38, 73 and 94, Briscoe discloses a method further comprising the steps of:

storing the group session key associated with the multicast group in a directory of the directory service [0058-0060];

authenticating a first multicast proxy service node with a subset of multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory [0058-0060];

receiving a plurality of private keys from the subset of multicast proxy service nodes [0058-0060];



receiving the new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a directory system agent (DSA) of a local multicast proxy service node that has received the new group session key through periodic replication of the directory by a replication service agent (RSA) of the local multicast proxy service node, wherein the RSA is signaled to carry out replication by storing an updated group session key in a local node of the director [0058-0060];

communicating the new group session key to the first multicast proxy service node [0058-0060];

communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys [0058-0060].

As to claims 42, 74 and 95, Briscoe discloses a method further comprising the steps of:

distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory [0058-0060];

replicating the directory [0058-0060]; and

obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node [0058-0060].

As to claim 47, 75 and 96, Briscoe discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents [0092-0109];

establishing a secure back channel group among the plurality of multicast service agents [0092-0109];

updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group [0092-0109];

at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of the each intermediate node [0092-0109].

As to claims 48, 76 and 97, Briscoe discloses a method further comprising the steps of:

receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree [0130-0140];

determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain [0130-0140];

establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with

a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain [0130-0140].

As to claims 51, 77 and 98, Briscoe discloses a method further comprising the step of managing removal of a first member node from the multicast group, wherein managing removal of the first member node further comprises the steps of:

creating and storing the group session key associated with the multicast group and a private key associated with each member node of the plurality of member nodes in a directory [0058-0060];

receiving information indicating that the first member node is leaving the multicast group [0058-0060];

updating all affected keys of a subset of member nodes of the plurality of member nodes in a branch of the second binary tree that contains the first member node that is leaving [0058-0060];

receiving the new group session key for the multicast group, for use after removal of the first member node, and a new private key for a parent node of the first member node, from a local multicast proxy service node of the plurality of multicast proxy service nodes [0058-0060];

communicating a message to the subset of member nodes that causes the subset of member nodes to update their private keys [0058-0060].

As to claims 54, 78 and 99, Briscoe discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents [0141-0149];

establishing a secure back channel group among the plurality of multicast service agents [0141-0149];

updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group [0141-0149];

at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of the each intermediate node [0141-0149].

As to claims 55, 79 and 100, Briscoe discloses a method further comprising the steps of:

receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree [0167-0179];

determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain [0167-0179];

establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with

a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain [0167-0179].

As to claims 56, 80 and 101, Briscoe discloses a method further comprising the steps of:

distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory [0058-0060];

replicating the directory [0058-0060]; and

obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node [0058-0060].

As to claim 59, Briscoe discloses a computer-readable medium carrying one or more sequences of instructions for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving information defining a plurality of multicast proxy service nodes [0058], wherein:

the plurality of multicast service nodes are distributed across the wide area network [0058];

the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group [0077]; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree [0114], wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network [0125-0129]; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes [0125-0129];

creating and storing a second binary tree that represents the plurality of member nodes [0125-0129], wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree [0131-0135];

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network [0131-0135];

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes [0131-0135]; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center [0131-0135];

creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange [0131-0135];

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree [0131-0135].

As to claim 60, Briscoe discloses a communication system for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, the communication system comprising:

a plurality of multicast proxy service nodes [0058], wherein:

the plurality of multicast service nodes are distributed across the wide area network [0058];

the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group [0077]; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree [0114], wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network [0125-0129]; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes [0125-0129];

a computer-readable medium comprising one or more instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

creating and storing a second binary tree that represents the plurality of member nodes [0125-0129], wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree [0131-0135];

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network [0131-0135];

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes [0131-0135]; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center [0131-0135];



creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange [0131-0135];

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree [0131-0135].

As to claim 81, Briscoe discloses an apparatus for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, the apparatus comprising:

means for receiving information defining a plurality of multicast proxy service nodes [0058], wherein:

the plurality of multicast service nodes are distributed across the wide area network [0058];

the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group [0077]; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree [0114], wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network [0125-0129]; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes [0125-0129];

means for creating and storing a second binary tree that represents the plurality of member nodes [0125-0129], wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree [0131-0135];

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network [0131-0135];

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes [0131-0135]; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center [0131-0135];

means for creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange [0131-0135];

means for determining a new group session key by replicating a branch of the second binary tree when an additional member node joins the multicast group [0131-0135].

*Conclusion*

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy   
March 30, 2006

CHRISTOPHER REVAK  
PRIMARY EXAMINER

 4/2/06